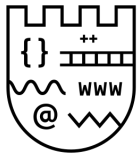
Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης

Σχολή Θετικών Επιστημών



ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Εργασία στο μάθημα της Κρυπτογραφίας

Φτιάκας Σωτήριος ΑΕΜ: 3076

Μπάρμπας Γρηγόριος ΑΕΜ: 3108

4 Ιουνίου 2020

Περιεχόμενα

Περίληψη

.....

Θέμα 1

RC4 & OTP

Κώδικας με σχόλια στα αρχεία:

No1_i_RC4.ipynb

No1_ii_OTP.ipynb

Θέμα 2

Avalanche Effect

Κώδικας με σχόλια στο αρχείο:

No2_Avalanche_Effect.ipynb

Θέμα 3

Vigenere

Κώδικας με σχόλια στο αρχείο:

No3_Vigenere.ipynb

Θέμα 4

K,Y,E

Ο αριθμός κάθε γράμματος που βρίσκεται στα αριστερά προστίθεται στον αντίστοιχο αριθμό του κλειδιού, το αποτέλεσμα ανάγεται σε mod 26 και αντικαθίσταται από το γράμμα του πίνακα.

Για παράδειγμα, έστω ότι το πρώτο γράμμα είναι το x. Προσθέτοντας με πιθανό κλειδί K = 11, έχουμε x+11. Αφού είναι 26 τα γράμματα της αγγλικής αλφαβήτας, κάνουμε x+11 mod 26. Αυτό όπως βλέπουμε μας δίνει το A σαν κρυπτογραφημένο μήνυμα, το οποίο ισούται με 1. Επομένως x+11 mod 26 = 1. Η λύση λοιπόν για x ανάμεσα στο 1 και το 26 είναι x = 16, με 16ο γράμμα της αλφαβήτας να είναι το P. Για πιθανό κλειδί E = 5, το x = 22, άρα το γράμμα είναι το V. Για πιθανό κλειδί το Y = 25, το x = 2, άρα το γράμμα είναι το B. Παρόμοια συνεχίζουμε για κάθε κρυπτογραφημένο γράμμα.

Μετά από παρατήρηση, το τελικό αποκρυπτογραφημένο μήνυμα είναι το PEACE BEGINS WITH A SMILE.

	K = 11	E = 5	Y = 25
A = 1	**P**	V	B
J = 10	Y	**E**	K
Z = 0	O	U	**A**
B = 2	Q	W	**C**
P = 16	**E**	K	Q
M = 13	**B**	H	N
D = 4	S	Y	**E**
L = 12	A	**G**	M
H = 8	W	C	**I**
Y = 25	**N**	T	Z
D = 4	**S**	Y	E
B = 2	Q	**W**	C
T = 20	**I**	O	U
S = 19	H	N	**T**
M = 13	B	**H**	N
F = 6	U	**A**	G
D = 4	**S**	Y	E
X = 24	**M**	S	Y
T = 20	**I**	U	U
Q = 17	F	**L**	R
J = 10	Y	**E**	K

Θέμα 5

Dictionary Attack

Κώδικας με σχόλια στο αρχείο:

No5_DictionaryAttack.ipynb

Θέμα 6

LSFR

Κώδικας με σχόλια στο αρχείο:

No6_LSFR.ipynb

Θέμα 7

Shift Operator with XOR

m: 16-bits

$$c = m \oplus (m << 6) \oplus (m << 10)$$

Όπου $m << a$ είναι κύλιση προς τα αριστερά κατά a-bits.

Για μήνυμα m και κλειδί k ισχύει: Αν $c = m \oplus k$, τότε $m = c \oplus k$

Επιπλέον, στην αρχική μας συνάρτηση κρυπτογράφησης, μπορούμε να κυλίσουμε και τα δύο μέλη ταυτόχρονα.

$$(c << 2) = (m \oplus (m << 6) \oplus (m << 10)) << 2$$

$$\Leftrightarrow (c << 2) = (m << 2) \oplus (m << 8) \oplus (m << 12)$$

Σημείωση: το $x << i$ θα συμβολίζεται ως x_i για ευκολία.
Συνεπώς θα έχουμε:

$$c_0 = m_0 \oplus m_6 \oplus m_{10} \quad (1)$$

$$c_2 = m_2 \oplus m_8 \oplus m_{12} \Rightarrow m_8 = m_2 \oplus m_{12} \oplus c_2 \quad (4)$$

$$c_4 = m_4 \oplus m_{10} \oplus m_{14} \Rightarrow m_{10} = m_4 \oplus m_{14} \oplus c_4 \quad (2)$$

$$c_6 = m_6 \oplus m_{12} \oplus m_0 \quad (5)$$

$$c_8 = m_8 \oplus m_{14} \oplus m_2$$

$$c_{10} = m_{10} \oplus m_0 \oplus m_4$$

$$c_{12} = m_{12} \oplus m_2 \oplus m_6$$

$$c_{14} = m_{14} \oplus m_4 \oplus m_8 \Rightarrow m_{14} \oplus m_4 = m_8 \oplus c_{14} \quad (3)$$

Ξεκινώντας από την (1) έχουμε διαδοχικά:

$$c_0 = m_0 \oplus m_6 \oplus m_{10}$$

$$(2) \Rightarrow c_0 = m_0 \oplus m_6 \oplus m_4 \oplus m_{14} \oplus c_4$$

$$(3) \Rightarrow c_0 \oplus c_4 = m_0 \oplus m_6 \oplus m_8 \oplus c_{14}$$

$$(4) \Rightarrow c_0 \oplus c_4 \oplus c_{14} = m_0 \oplus m_6 \oplus m_2 \oplus m_{12} \oplus c_2$$

$$(5) \Rightarrow c_0 \oplus c_4 \oplus c_{14} \oplus c_2 = m_2 \oplus c_6$$

$$\Rightarrow c_0 \oplus c_4 \oplus c_{14} \oplus c_2 \oplus c_6 = m_2 \quad (6)$$

Κάνουμε κύλιση και στα δύο μέρη του (6) προς τα δεξιά και έχουμε:

$$m_0 = c_{14} \oplus c_2 \oplus c_{12} \oplus c_0 \oplus c_4$$

και άρα τελικά έχουμε:

$$m_0 = c_0 \oplus c_2 \oplus c_4 \oplus c_{12} \oplus c_{14}$$

Κώδικας με σχόλια στο αρχείο:

No7_Shift_Operator.ipynb

Θέμα 8

GCD Greatest Common Divisor

(i) Διαιρώ το 126048 με το 5050 και έχω $126048 = 5050 \cdot 24 + 4848$. Κατόπιν διαιρώ τον διαιρέτη, δηλαδή το 5050 με το υπόλοιπο, δηλαδή με το 4848 και

έχουμε $5050 = 4848 \cdot 1 + 202$. Τέλος, συνεχίζοντας όπως προηγουμένως έχω $4848 = 24 \cdot 202 + 0$. Το τελευταίο μη μηδενικό υπόλοιπο, δηλαδή το 202 είναι ο ΜΚΔ των αριθμών.

Για τους αριθμούς Bezout έχουμε:

$202 = 5050 - 4848 = 5050 - (126048 - 24 \cdot 5050) = \mathbf{-1} \cdot 126048 + \mathbf{25} \cdot 5050$

Άρα, οι αριθμοί Bezout είναι οι: **-1**, **25**

$Z_{1001}, x = 809$

(ii)

$$1001 = 809 \cdot 1 + 192$$

$$809 = 192 \cdot 4 + 41$$

$$192 = 41 \cdot 4 + 28$$

$$41 = 28 \cdot 1 + 13$$

$$28 = 13 \cdot 2 + 2$$

$$13 = 2 \cdot 6 + 1$$

$$1 = 13 - 2 \cdot 6 =$$

$$13 - (28 - 13 \cdot 2) \cdot 6 =$$

$$13 \cdot 13 - 28 \cdot 6 =$$

$$13 \cdot (41 - 281) - 28 \cdot 6 =$$

$$13 \cdot 41 - 28 \cdot 13 - 28 \cdot 6 =$$

$$13 \cdot 41 + 28 \cdot (-19) =$$

$$13 \cdot 41 + (192 - 41 \cdot 4) \cdot (-19) =$$

$$13 \cdot 41 + 192 \cdot (-19) + 41 \cdot 76 =$$

$$89 \cdot 41 + 192 \cdot (-19) =$$

$$89 \cdot (809 - 192 \cdot 4) + 192 \cdot (-19) =$$

$$89 \cdot 809 - 192 \cdot 356 + 192 \cdot (-19) =$$

$$89 \cdot 809 + 192 \cdot (-375) =$$

$$89 \cdot 809 + (1001 - 809 \cdot 1) \cdot (-375) =$$

$$89 \cdot 809 + 1001 \cdot (-375) + 809 \cdot (375) =$$

$$464 \cdot 809 + 1001 \cdot (-375)$$

$$1 \equiv 464 \cdot 809 \mod 1001$$

Άρα το αντίστροφο του 809 στο Z_{1001} είναι το 464.

(iii) Ξέρουμε από το μικρό θεώρημα του Fermat ότι:

$$n^{p-1} \equiv 1 \mod p$$

δηλαδή $2^{100} \equiv 1 \mod 101$

άρα $2^{100} \equiv 1$

Θέμα 9

Entropy

Αρχικά υπολογίζουμε

$$p_x(X=0) = \sum_y p_{X,Y}(0,y) = \frac{3}{7}$$
$$p_x(X=1) = \sum_y p_{X,Y}(1,y) = \frac{2}{7}$$
$$p_x(X=2) = \sum_y p_{X,Y}(2,y) = \frac{2}{7}$$
$$p_y(Y=0) = \sum_y p_{X,Y}(x,0) = \frac{3}{7}$$
$$p_y(Y=1) = \sum_y p_{X,Y}(x,1) = \frac{2}{7}$$
$$p_y(Y=2) = \sum_y p_{X,Y}(x,2) = \frac{2}{7}$$

Ισχύει ότι:

$$H(X) = -\sum_x p_X(x) \log_2 p_X(x)$$

Επομένως

$$\begin{aligned} H(X) &= -\frac{3}{7}\log_2\frac{3}{7} - \frac{2}{7}\log_2\frac{2}{7} - \frac{2}{7}\log_2\frac{2}{7} \\ &= -\frac{3}{7}\log_2\frac{3}{7} - \frac{4}{7}\log_2\frac{2}{7} \\ &\simeq 1.5566567074628228 \end{aligned}$$

$$\begin{aligned} \Upsilon(Q) &= -\frac{3}{7}\log_2\frac{3}{7} - \frac{2}{7}\log_2\frac{2}{7} - \frac{2}{7}\log_2\frac{2}{7} \\ &= -\frac{3}{7}\log_2\frac{3}{7} - \frac{4}{7}\log_2\frac{2}{7} \\ &\simeq 1.5566567074628228 \end{aligned}$$

Επίσης έχουμε τον εξής τύπο

$$H(X, Y) = -\sum_x \sum_y p(x, y)\log_2 p(x, y)$$

Άρα θα έχουμε:

$$\begin{aligned} H(X, \Upsilon) = &-p(0,0)\log_2 p(0,0) - p(0,1)\log_2 p(0,1) - p(0,2)\log_2 p(0,2) - \\ &p(1,0)\log_2 p(1,0) - p(1,1)\log_2 p(1,1) - p(1,2)\log_2 p(1,2) - \\ &p(2,0)\log_2 p(2,0) - p(2,1)\log_2 p(2,1) - p(2,2)\log_2 p(2,2) \\ &\simeq 2.5216406363433186 \end{aligned}$$

Θα υπολογίσουμε την $H(Y|X)$. Χρειαζόμαστε αρχικά τα παρακάτω,

$$p_{Y|X}(y=0|x=0) = \frac{p_{X,Y}(0,0)}{p_X(0)} = \frac{\frac{1}{7}}{\frac{3}{7}} = \frac{1}{3}$$

$$p_{Y|X}(y=1|x=0) = \frac{p_{X,Y}(0,1)}{p_X(0)} = \frac{0}{\frac{3}{7}} = 0$$

$$p_{Y|X}(y=2|x=0) = \frac{p_{X,Y}(0,2)}{p_X(0)} = \frac{\frac{2}{7}}{\frac{3}{7}} = \frac{2}{3}$$

$$p_{Y|X}(y=0|x=1) = \frac{p_{X,Y}(1,0)}{p_X(1)} = \frac{\frac{1}{7}}{\frac{2}{7}} = \frac{1}{2}$$

$$p_{Y|X}(y=1|x=1) = \frac{p_{X,Y}(1,1)}{p_X(1)} = \frac{\frac{1}{7}}{\frac{2}{7}} = \frac{1}{2}$$

$$p_{Y|X}(y=2|x=1) = \frac{p_{X,Y}(1,2)}{p_X(1)} = \frac{0}{\frac{2}{7}} = 0$$

$$p_{Y|X}(y=0|x=2) = \frac{p_{X,Y}(2,0)}{p_X(2)} = \frac{\frac{1}{7}}{\frac{2}{7}} = \frac{1}{2}$$

$$p_{Y|X}(y=1|x=2) = \frac{p_{X,Y}(2,1)}{p_X(2)} = \frac{\frac{1}{7}}{\frac{2}{7}} = \frac{1}{2}$$

$$p_{Y|X}(y=2|x=2) = \frac{p_{X,Y}(2,2)}{p_X(2)} = \frac{0}{\frac{2}{7}} = 0$$

Τώρα πρέπει να υπολογίσουμε τα παρακάτω:

$$
\begin{aligned}
H(Y|X=0) &= -\sum_y p_{Y|X}(y|x=0)\log_2 p_{Y|X}(y|x=0) \\
&= -(\frac{1}{3}\log_2\frac{1}{3} + 0 + \frac{2}{3}\log_2\frac{2}{3}) \\
&= -(\frac{1}{3}\log_2\frac{1}{3} + \frac{2}{3}\log_2\frac{2}{3}) \\
H(Y|X=1) &= -\sum_y p_{Y|X}(y|x=1)\log_2 p_{Y|X}(y|x=1) \\
&= -(\frac{1}{2}\log_2\frac{1}{2} + \frac{1}{2}\log_2\frac{1}{2} + 0) \\
&= -\log_2 2 = 1 \\
H(Y|X=2) &= -\sum_y p_{Y|X}(y|x=2)\log_2 p_{Y|X}(y|x=2) \\
&= -\log_2 2 = 1
\end{aligned}
$$

Τότε θα έχουμε

$$
\begin{aligned}
H(Y|X) &= \sum_x p_X x H(Y|X=x) \\
&= p_X(0)H(Y|X=0) + p_X(1)H(Y|X=1) + p_x(2)H(Y|X=2) \\
&\simeq 0.9649839288804954
\end{aligned}
$$

Γνωρίζουμε επίσης ότι από το θεώρημα της αμοιβαίας πληροφορίας έχουμε

$$I(X,Y) = H(X) - H(X|Y) = H(Y) - H(Y|X)$$

΄Αρα έχουμε

$$H(X|Y) = -(H(Y) - H(Y|X) - H(X))$$
$$\simeq 0.9649839288804954$$

Τέλος,

$$\rho = 1 - \frac{H(Y|X)}{H(X)}$$
$$\simeq 0.5916727785823274$$

Κώδικας με σχόλια στο αρχείο:

No9_Entropy.ipynb

Θέμα 10

Textbook RSA

Κώδικας με σχόλια στο αρχείο:

No10_Textbook_RSA.ipynb

Θέμα 11

Wiener RSA

Κώδικας με σχόλια στο αρχείο:

No11_Wiener_RSA.ipynb

Θέμα 12

Prime Numbers

Κώδικας με σχόλια στο αρχείο:

No12_Prime_Numbers.ipynb

Θέμα 13

Chinese Theorem

Έχουμε το σύστημα των γραμμικών ισοδυναμιών

$$x \equiv 9 \pmod{19}$$
$$x \equiv 9 \pmod{12}$$
$$x \equiv 13 \pmod{19}$$

Έχουμε ότι ισχύει $\gcd(12, 17, 19) = 1$, άρα δεν απαιτείται κάποια απλοποίηση.

Για την επίλυση του συστήματος χρησιμοποιούμε το Κινέζικο Θεώρημα Υπολοίπων

Έτσι έχουμε: $m = 17 * 12 * 19 = 3876$

$$
\begin{aligned}
M_1 = 228y_1 \equiv 1 \mod 17 &\implies 7y_1 \equiv \mod 17 \implies y_1 = 5 \\
M_2 = 323y_2 \equiv 1 \mod 12 &\implies 11y_1 \equiv \mod 12 \implies y_1 = 11 \\
M_3 = 204y_3 \equiv 1 \mod 19 &\implies 14y_1 \equiv \mod 19 \implies y_1 = 15
\end{aligned}
$$

Τώρα πολλαπλασιάζουμε και προσθέτουμε:

$$
\begin{aligned}
x &= 9 * 228 * 5 + 9 * 323 * 11 + 13 * 204 * 15 \\
&= 82017(1)
\end{aligned}
$$

Παρατηρούμε ότι η (1) γράφεται,

$$x = 82017 = 621 + 3876k, k \in \mathbb{Z}$$

Για $k = 0$ έχουμε λύση το $x = 621$

Κώδικας με σχόλια στο αρχείο:

*No*13_*ChineseTheorem*.*ipynb*

Θέμα 14

Miller-Rabin Test

1. We can see that a big portion of the total numbers generated from $f(x) = x^2 + x - 1354363$, about 2/5 of the total, are primes

2. A lucky number of Euler is a number p such that the prime-generating polynomial:
   $n^2 - n + p$ is prime for $n = 1, 2, \ldots, p - 1$

   Specifically, the lucky numbers of Euler (excluding the trivial case $p = 3$) are those numbers p such that the imaginary quadratic field Q(sqrt(1-4p)) has class number 1. (Rabinowitz 1913, Le Lionnais 1983, Conway and Guy 1996, Ribenboim 2000).

   As proved by Heegner (1952) (although his proof was not accepted as complete at the time) and subsequently established by Stark (1967), there are only nine numbers -d such that h(-d)=1 (the Heegner numbers -2, -3, -7, -11, -19, -43, -67, and -163), and of these, only 7, 11, 19, 43, 67, and 163 are of the required form.

   Therefore, the only lucky numbers of Euler are 2, 3, 5, 11, 17, and 41 (Le Lionnais 1983, OEIS A014556), and **there does not exist a better prime-generating polynomial of Euler's form**.

Κώδικας με σχόλια στο αρχείο:

No12_Miller – Rabin_Test.ipynb

Θέμα 15

Rabin TDF

Κώδικας με σχόλια στο αρχείο:

*No*15_*Rabin_TDF.ipynb*

Θέμα 16

GPG, PGP, Send Message

Μπάρμπας Γρηγόριος:

$b641ed06419f8ff4a6447cc9fb9d2295$

Φτιάκας Σωτήριος:

$5f816b4f295dc95721a7a34b9fd1653a$

Θέμα 17

TDF: CRT-RSA

Κώδικας με σχόλια στο αρχείο:

No17_TDF_CRT – RSA.ipynb

Θέμα 18

secure.zip

9e94b15ed312fa42232fd87a55db0d39

Θέμα 19

OpenSSL

Κώδικας με σχόλια στο αρχείο:

No19_OpenSSL.ipynb

Θέμα 20

/dev/random

Κώδικας με σχόλια στο αρχείο:

No12_dev_random_entropy.ipynb

Θέμα 21

Bibliography

1. **Να αναλύσετε πως η χρήση του ίδιου κλειδιού στον OTP επιτρέπει να βρούμε μηνύματα που είναι γραμμένα σε κάποια φυσική γλώσσα.**
   Το OTP αποτελεί ένα stream cipher ο οποίος αποτελεί μια perfectly secure μέθοδο κρυπτογράφησης. Είναι πολύ εύκολος στην υλοποίησή του και είναι perfectly secure εάν το μήκος του κλειδιού που χρησιμοποιείται είναι μεγαλύτερο ή ίσο του μήκους του μηνύματος που κρυπτογραφείται. Ωστόσο, απαιτεί επίσης το κλειδί να μην χρησιμοποιηθεί πάνω από μία φορά. Ας δούμε ένα παράδειγμα του πως μπορούμε να εξάγουμε πληροφορία από δύο κρυπτογραφημένα μηνύματα που έχουν κρυπτογραφηθεί χρησιμοποιώντας το ίδιο κλειδί. Έστω ότι έχουμε τα εξής:

   - message1 = "Hello World"
   - message2 = "the program"
   - key = "supersecret"

Αν μετατρέψουμε κάθε μήνυμα σε ηεξ στρινγς, και τα κρυπτογραφήσουμε χρησιμοποιώντας το ίδιο κλειδί, θα πάρουμε τα εξής cipher-texts:

- cipher-text1: "3b101c091d53320c000910"
- cipher-text2: "071d154502010a04000419"

Ακολουθούμε λοιπόν την εξής διαδικασία:

(α΄) Μαντεύουμε μια λέξη που μπορεί να υπάρχει σε κάποιο από τα αρχικά μηνύματα.

(β΄) Μετατρέπουμε τη λέξη σε hex string.

(γ΄) Κάνουμε XOR τα δύο cipher-texts.

(δ΄) Κάνουμε XOR το hex string που δημιουργήσαμε στο βήμα 2 με το hex string που δημιουργήσαμε στο βήμα 3.

(ε΄) Αν το αποτέλεσμα είναι λέξη φυσικής γλώσσας, τότε έχουμε καταφέρει να αποσπάσουμε πληροφορία και για τα δύο αρχικά μηνύματα.

(Ϛ΄) Αν δεν είναι λέξη φυσικής γλώσσας, τότε συνεχίζουμε να κάνουμε XOR, μετακινόντας τη λέξη μας κάθε φορά ένα βήμα δεξιά.

Το βήμα 1 φαίνεται δύσκολο, δηλαδή το να μαντέψουμε κάποια λέξη σε κάποιο από τα δύο κείμενα, αλλά αν σκεφτούμε έξυπνα, μπορούμε να βελτιώσουμε τις πιθανοτητές μας. Για παράδειγμα, η λέξη "the" αποτελεί την πιο συχνά χρησιμοποιούμενη λέξη. Θα υποθέσουμε λοιπόν ότι υπάρχει σε ένα από τα μηνύματα.

Από βήμα 2: Η λέξη "the" μετατρέπεται ως hex string σε ¨746865¨.

Από βήμα 3: $cipher-text1 \quad XOR \quad cipher-text2 =$ ”3c0d094c1f523808000d09”

Από βήμα 4:

$$3c0d094c1f523808000d09$$

$$XOR \quad 746865$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

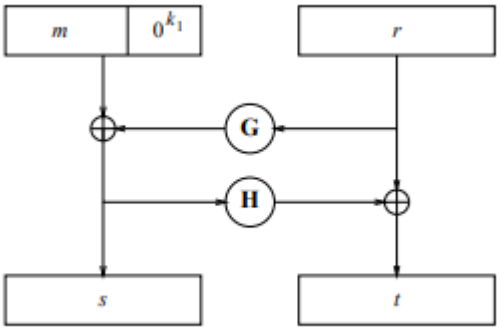
$$48656c$$

Αν μετατρέψουμε το “48656c” σε ASCII, παίρνουμε το μήνυμα "Hel". Αυτό μας πηγαίνει στο **βήμα 5**. Επειδή μοιάζει με λέξη φυσική γλώσσας, μπορούμε να υποθέσουμε ότι το "the" υπάρχει στην πρώτη θέση κάποιου μηνύματος. Αν δεν βρίσκαμε λέξη φυσικής γλώσσας, θα μετακινούσαμε σύμφωνα με το **βήμα 6**, το "48656c" μια θέση δεξιά και θα δοκιμάζαμε ξανά.

Από εκεί και πέρα, δοκιμάζοντας και ¨μαντέυοντας¨ λέξεις που αρχίζουν από "Hel" όπως π.χ. "Help", "Hello" κτλ, με την ίδια ακριβώς διαδικασία, μπορούμε να αποσπάσουμε και άλλη πληροφορία από τα δύο μηνύματα.

Συμπεραίνουμε λοιπόν ότι η επαναχρησιμοποίηση του ίδιου κλειδιού στο OTP κρύβει κινδύνους.
ref: many-time-pad-attack-crib-drag

2. **Να αναλύσετε πως δουλέυει το RSA-OAEP**
   Το OAEP προέρχεται από την ονομασία Optimal Asymmetric Encryption Padding και αποτελεί ένα σχήμα κρυπτογράφησης που χρησιμοποιεί paddings και είναι βασισμένο στο RSA. Ο τρόπος με τον οποίο λειτουργεί μπορεί να αναπαρασταθεί εύκολα με το παρακάτω σχεδιάγραμμα:



Αναλυτικότερα, έχουμε τα εξής:

- **G**: μία hash function με output g bits
- **H**: μία hash function με output h bits
- **r**: μία συμβολοσειρά μήκους g bits

Έστω **m** το μήνυμα που θέλουμε να κρυπτογραφήσουμε με μήκος bits μικρότερο από g bits.

Αρχικά, δημιουργούμε το καινούριο μήνυμα **m'**, το οποίο αποτελεί το παλιό μήνυμα m στο οποίο έχουμε προσθέσει στο τέλος (έχουμε κάνει **append**) όσα **μηδενικά** χρειάζεται για να φτάσουμε το νέο μήνυμα **να είναι μήκους g bits**.

Στη συνέχεια δημιουργούμε:

- Το **s** το οποίο παράγεται κάνοντας: **m' XOR G(r)**.
- Το **t** το οποίο παράγεται κάνοντας: **r XOR H(m' XOR G(r))**.

Τέλος, δημιουργούμε το **X** το οποίο αποτελεί την ένωση του **s** || **t** (δηλαδή s append t), και μετά κρυπτογραφούμε το X χρησιμοποιώντας το **RSA** και στέλνουμε το κρυπτογραφημένο μήνυμά μας.

ref: 2002-cryptobytes

3. **Να μελετήσετε βιβλιογραφικα τις στρατηγικές first sign then encrypt & first encrypt then sign και να καταλήξετε σε κάποια συμπεράσματα (πλεονεκτήματα/μειονεκτήματα)**

   - Κατα την στρατηγική **first sign then encrypt**, η λογική είναι η εξής:

   Ο αποστολέας μαζί με το μήνυμά του, βάζει επίσης την ψηφιακή υπογραφή του. Στη συνέχεια, και τα δύο αυτά μαζί τα κρυπτογραφεί και τα στέλνει σε κάποιον παραλήπτη.

   - Κατα την στρατηγική **first encrypt then sign**, η λογική είναι η εξής:

   Ο αποστολέας κρυπτογραφεί το μήνυμά του, στη συνέχεια βάζει την ψηφιακή υπογραφή του μαζί με το κρυπτογραφημένο πια μήνυμα και τα στέλνει σε κάποιον παραλήπτη.

   Ανάλυση
   Όταν χρησιμοποιούμε την **first sign then encrypt** στρατηγική, είναι προφανές ότι η ψηφιακή μας υπογραφή στέλνεται και αυτή κρυπτογραφημένη στον παραλήπτη. Αυτό σημαίνει πρακτικά ότι μόνο ο παραλήπτης μπορεί να αποκρυπτογραφήσει το μήνυμα και μετά να επιβεβαιώσει την ψηφιακή υπογραφή μου, ενώ αν κάποιος τρίτος πάρει στα χέρια του το cipher-text, δεν μπορεί να βγάλει κανένα συμπέρασμα ούτε για το μήνυμα ούτε για το ποιανού είναι η υπογραφή.

   Όταν χρησιμοποιούμε την **first encrypt then sign** στρατηγική ωστόσο, η ψηφιακή μας υπογραφή στέλνεται μη-κρυπτογραφημένη μαζί με το κρυπτογραφημένο μήνυμα στον παραλήπτη. Αυτό σημαίνει ότι αν κάποιος τρίτος πάρει στα χέρια του το cipher-text του μηνύματος μαζί με την υπογραφή μου, μπορεί να δει ότι κάτι έχω υπογράψει αλλά δεν μπορεί φυσικά να δει το περιεχόμενο του μηνύματος.

Συμπεράσματα

Καταλήγουμε λοιπόν στο συμπέρασμα ότι δεν υπάρχει σωστή η λάθος στρατηγική ανάμεσα στις δύο, καθώς εξαρτάται από το τι θέλουμε να πετύχουμε. Η κοινή λογική λέει πως από τι στιγμή που στέλνουμε ένα κρυπτογραφημένο κείμενο σε κάποιον, θέλουμε ένας τρίτος που πάρει στα χέρια του το cipher text να έχει όσο δυνατόν λιγότερη πληροφορία για αυτό, και άρα η στρατηγική **first sign then encrypt** φαντάζει πιο σωστή.

Για παράδειγμα, αν έχω χρησιμοποιήσει την στρατηγική **first encrypt then sign** και κάποιος τρίτος πάρει στα χέρια του το cipher text με την υπογραφή μου που έστειλα στον παραλήπτη X, μπορεί να αλλάξει την υπογραφή μου, να εισάγει την υπογραφή του, και να στείλει το cipher text στον παραλήπτη X ως δικό του. Αυτό ελλωχεύει τον κίνδυνο ο X να έρθει σε επαφή με τον τρίτο, καθώς νομίζει ότι αυτός του έστειλε το cipher-text που αρχικά έστειλα εγώ, και να του αποκαλύψει άθελά του πληροφορίες για το αποκρυπτογραφημένο μήνυμα.

Ο μόνος λόγος για να χρησιμοποιήσουμε την στρατηγική **first encrypt then sign** θα ήταν εάν δεν θα μας πείραζε ή ακόμη καλύτερα αν θα θέλαμε να φαίνεται σε όλους, σε οποιονδήποτε μπορεί να πάρει το cipher-text, ότι το μήνυμα αυτό το έχω υπογράψει εγώ.

Θέμα 22

3.1

Αρχικά θέλουμε να αποδείξουμε ότι οι αριθμοί της μορφής $4n+3$ δεν είναι τέλεια τετράγωνα. Αρχικά για $n \leq 0$ εύκολα παρατηρούμε ότι ισχύει η παραπάνω πρόταση. Αυτό συμβαίνει καθώς για $n = 0$ έχουμε το 3 το οποίο δεν είναι τέλειο τετράγωνο

και για $n < 0$ το $4n + 3$ είναι αρνητικός.

Έστω ότι,

$$4n + 3 = a^2, \quad n, a \in \mathbb{N}^*(1)$$

Εφόσον $a \in \mathbb{N}^*$, τότε μπορούμε να πούμε ότι $a = 2k + 1, \quad k \in \mathbb{N}$.

Αντικαθιστώντας το a στην (1) έχουμε:

$$\begin{aligned} 4n + 3 = (2k + 1)^2 &\implies 4n + 3 = 4k^2 + 4k + 1 \\ &\equiv 4k^2 + 4k - 4n = 2 \\ &\equiv 2(k^2 + k - n) = 1 \\ &\equiv k^2 + k - n = \frac{1}{2} \end{aligned}$$

Το οποίο είναι άτοπο καθώς $k, n \in \mathbb{N}^*$ και άρα το $k^2 \in \mathbb{N}^*$ αλλά και όλη η παράσταση $k^2 + k - n \in \mathbb{N}$, εφόσον είναι άθροισμα των φυσικών αριθμών k^2, k και $-n$.

Συνεπώς και η αρχική ισοδύναμη υπόθεση είναι άτοπη, οπότε το $4n+3$ δεν είναι τέλειο τετράγωνο.

Για το δεύτερο ερώτημα παρατηρούμε ότι όλοι αριθμοί

$$11, 111, \ldots, 111\cdots111, \ldots$$

μπορούν να γραφούν στην μορφής $(4n + 3) + 10^q$, συνεπώς αυτό το σύνολο αριθμών δεν θα έχει τέλειο τετράγωνο.

Θέμα 23

3.4

Υπάρχουν δύο περιπτώσεις που θα χρειαστεί να εξετάσουμε.

Περίπτωση 1: Για περιττό αριθμό διαδοχικών αριθμών, αυτοί οι αριθμοί θα

έχουν ως μέσο έναν ακέραιο (μεσσαίος αριθμός), οπότε το άθροισμα γράφεται ως εξής:

$$sum = average * number\_of\_consecutive\_numbers$$

$$\implies sum = integer * odd\_number$$

Αυτό σημαίνει ότι το άθροισμα (sum) διαιρείται από έναν περιττό αριθμό. Αυτό όμως δεν μπορεί να είναι το σενάριο για το 2^m.

Περίπτωση 2: Ένας ζυγός αριθμός διαδοχικών αριθμών έχουν ως μέσο το μέσο του αθροίσματος των δύο μεσαίων. Συνεπώς έχουμε:

$$sum = ((sum\_of\_two\_middle\_numbers) * \frac{1}{2}) * number\_of\_consecutive\_numbers$$

$$\implies sum = (sum\_of\_two\_middle\_numbers) * \frac{1}{2} * even\_number$$

$$\implies sum = (sum\_of\_two\_middle\_numbers) * integer$$

$$\implies sum = ((k) + (k+1)) * integer \quad , k \in \mathbb{Z}$$

$$\implies sum = (2k+1) * integer$$

Το $2k+1$ είναι περιττός αριθμός, άρα το άθροισμα (sum) έχει ως παράγοντα περιττό, άρα όπως και προηγουμένως απορρίπτεται το σενάριο 2^m.

Θέμα 24

3.7

Έστω ότι

$$a = n^5 + 1, b = n^{10} - 1, c = n^5 - 1$$

$$a \cdot c = (n^5 + 1) \cdot (n^5 - 1) = n^{5^2} - 1^2 = n^{10} - 1 = b$$

Γνωρίζουμε όμως (από ορισμό 3.1.1) ότι $a|b$ αν υπάρχει ακέραιος αριθμός c τέτοιος ώστε $b = a \cdot c$. Επομένως, η αρχική πρόταση αποδείχτηκε.

Θέμα 25

3.19

Κώδικας με σχόλια στο αρχείο:

*No*25_*Maths*_3_19.*ipynb*

Θέμα 26

3.23

Από την εκφώνηση έχουμε δύο δεδομένα:

$$(1) \quad gcd(n, a) = 1$$

$$(2) \quad n|a \cdot b$$

Χρησιμοποιώντας το 1ο δεδομένο, από την ταυτότητα Bezout, υπάρχουν ακέραιοι x, y, τέτοιοι ώστε $1 = x \cdot n + y \cdot a$.
Οπότε $b = b \cdot x \cdot n + b \cdot y \cdot a$.
Αλλά:

$n|b \cdot x \cdot n$ (εννοείται) και

$n|y \cdot (a \cdot b)$ (χρησιμοποιώντας το 2ο δεδομένο)

Επομένως, $n|b \cdot x \cdot n + b \cdot y \cdot a$, δηλαδή $n|b$.

Θέμα 27

3.26

(i) Έστω ότι $d_1 = \gcd(c, b)$ και $d_2 = \gcd(ac, b)$

Τότε έχουμε $c \cdot x_1 + b \cdot y_1 = d_1$, $a \cdot c \cdot x_2 + b \cdot y_2 = d_2$ και $a \cdot x + b \cdot y = 1$, από Bezout. Αρχικά πολλαπλασιάζουμε την $a \cdot x + b \cdot y = 1$ με το d_1 και έχουμε:

$$\begin{aligned} & d_1 \cdot (a \cdot x + b \cdot y) = 1 \cdot d_1 \\ \implies & a \cdot x(c \cdot x_1 + b \cdot y_1) + b \cdot d_1 \cdot y = d_1 \\ \implies & a \cdot c \cdot (x \cdot x_1) + b \cdot (a \cdot x \cdot y_1 + d_1 \cdot y) = d_1 \end{aligned}$$

Εφόσον ισχύει ότι $d_2 = \gcd(ac, b)$, τότε διαιρεί κάθε ακέραιο γραμμικό συνδυασμό των ac και b και άρα έχουμε $d_2|d_1$ (1).

Στην συνέχεια θα πολλαπλασιάσουμε ομοίως το $a \cdot x + b \cdot y = 1$ με το d_2 και έχουμε:

$$\begin{aligned} & d_2 \cdot (a \cdot x + b \cdot y) = 1 \cdot d_2 \\ \implies & a \cdot x(a \cdot c \cdot x_2 + b \cdot y_2) + b \cdot d_2 \cdot y = d_2 \\ \implies & c \cdot (a^2 \cdot x \cdot x_2) + b \cdot (a \cdot x \cdot y_2 + d_2 \cdot y) = d_2 \end{aligned}$$

Ομοίως με προηγουμένως ισχύει ότι $d_1 = \gcd(c, b)$, τότε διαιρεί κάθε ακέραιο γραμμικό συνδυασμό των ac και b και άρα έχουμε $d_1|d_2$ (2). Από (1) και (2) έχουμε ότι $d_1 = d_2$, μη αρνητικά.

Αφού

$$(1) \implies |d_1| \leqslant |d_2|$$

$$(2) \implies |d_2| \leqslant |d_1|$$

(ii) Έστω d κοινός διαρέτης των $a+b$ και $a-b$, τότε ο d διαιρεί και το άθροισμα και την διαφορά τους.

$$d|(a+b)$$

$$d|(a-b)$$

$$d|(a+b)+(a+b) = 2\cdot a$$

$$d|(a+b)-(a-b) = 2\cdot b$$

Τότε έχουμε ότι:

$$d|\gcd(2a, 2b) = 2\gcd(a, b)$$

Όμως από αρχικά δεδομένα έχουμε ότι $\gcd(a, b) = 1$ άρα τότε ισχύει:

$$d|2$$

Συνεπώς το $d \in \{1, 2\}$

Εαν a,b περιττοί τότε έχουμε το εξής:

$$a = 2k_1 + 1 \quad k_1 \in \mathbb{Z}$$

$$b = 2k_2 + 1 \quad k_2 \in \mathbb{Z}$$

΄Αρα θα ισχύει και το εξής:

$$a + b = 2k_1 + 1 + 2k_2 + 1 = 2k_1 + 2k_2 + 2 = 2\cdot(k_1 + k_2 + 1) \quad (even)$$

$$a - b = 2k_1 + 1 - 2k_2 + 1 = 2k_1 - 2k_2 = 2 \cdot (k_1 - k_2) \quad (even)$$

Εφόσον και τα δύο είναι ζυγοί αριθμοί τότε οι διαιρέτες τους θα είναι ζυγοί. Όπως αποδείξαμε προηγούμενος όμως, αν d διαιρέτης, τότε $d \in \{1, 2\}$ Συμπερασματικά έχουμε ότι $d = 2$.

(iii) Έστω $d = \gcd(a, b)$ τότε $d = a \cdot x + b \cdot y, \quad x, y \in \mathbb{Z}$ Αν $i = \gcd(2^a - 1, 2^b - 1)$ τότε

$$2^a \equiv 1 \mod i$$

$$2^b \equiv 1 \mod i$$

Συνεπώς έχουμε

$$2^d = 2^{a \cdot x + b \cdot y} = (2^a)^x \cdot (2^b)^y \equiv 1 \mod i$$

Οπότε $p|2^d - 1$. Από την άλλη μεριά αν $d|a$, τότε $2^d - 1|2^q - 1$, οπότε το $2^d - 1$ αποτελεί κοινό παράγοντα. Έτσι αποδείξαμε ότι

$$\gcd(2^a - 1, 2^b - 1) = 2^{\gcd(a,b)} - 1$$

Όμως από αρχικά δεδομένα $d = 1$, άρα και η προηγούμενη σχέση γράφεται:

$$\gcd(2^a - 1, 2^b - 1) = 1$$

(iv) Παρατηρούμε ότι αν αντικαταστήσουμε τα M_p, M_q έχουμε την παραπάνω σχέση.

Θέμα 28

3.40

Κώδικας με σχόλια στο αρχείο:

No28_Maths_3_40.ipynb

Θέμα 29

3.42

Κώδικας με σχόλια στο αρχείο:

No29_Maths_3_42.ipynb

Θέμα 30

3.70

Υπόθεση:

$N > 2$

$N = p_1 p_2 \dots p_k$

$p_j - 1 | N - 1 \forall j$

Απόδειξη:

Έστω $\gcd(a, N) = 1$.

Από το θεώρημα του Fermat, $\forall j$, έχουμε $a^{p_j} \equiv 1 \mod p_j$.
Εφόσον $p_j - 1 | N - 1$,και άρα $a^{N-1} \equiv 1 \mod p_j$.
Δηλαδή το $a^{N-1} - 1$ είναι πολλαπλάσιο κάθε p_j.
Συνεπώς $a^{N-1} \equiv 1 \mod N$.

Θέμα 31

3.74

Παρατηρούμε ότι $561 (= 3 \cdot 11 \cdot 17)$ είναι αριθμός Carmichael. Θα βρούμε όλους του αριθμούς Carmichael μέχρι $N (= 3000)$.

Πρόταση 1: Έστω $n = p \cdot u$ όπου p είναι πρώτος. Τότε αν και μόνο αν $p - 1 | u - 1$ θα ισχύει και $p - 1 | n - 1$.

$$(n-1) - (u-1) = n - u = p \cdot u - u = (p-1) \cdot u$$

Πρόταση 2: Έστω ένας αριθμός Carmichael έχει τουλάχιστον τρεις πρώτους παράγοντες. Για την απόδειξη αυτής της πρότασης εφαρμόζουμε την εξής λογική:

Έστω ότι ο n έχει δύο πρώτους παράγοντες $n = p \cdot q$ όπου p, q πρώτοι και $p > q$. Τότε $p - 1 > q - 1$, άρα το $p - 1$ δεν διαιρεί το $q - 1$. Από την πρόταση (1) το $p - 1$ δεν διαιρεί το $n - 1$. Συνεπώς το n δεν είναι αριθμός Carmichael.

Πρόταση 3: Ας υποθέσουμε ότι ο n είναι Carmicael και ότι το p και το q είναι πρώτοι παράγοντες του n. Τότε $q \not\equiv 1 \mod p$.

Έστω ότι το $q \equiv 1 \mod p$, έτσι ισχύει ότι $p | q - 1$. Τότε $q - 1 | n - 1$ καθώς θα ισχύει και ότι $p | n - 1$. Όμως αυτό είναι άτοπο καθώς ισχύει ότι $p | n$.

Εύρεση αριθμών Carmichael: Έστω αριθμός n με τρεις πρώτους παράγοντες $n = p \cdot q \cdot r$, με $p < q < r$. Από τα προηγούμενα καταλαβαίνουμε ότι χρειαζόμαστε τριπλέτες (p, q, r) για τις οποίες θα ισχύουν τα εξής:

$$(i) \quad p-1|q\cdot r-1 \quad (or \quad q\cdot r\equiv 1 \mod (p-1))$$
$$(ii) \quad q-1|p\cdot r-1$$
$$(iii) \quad r-1|p\cdot q-1$$

Δοθεί ένα ζευγάρι πρώτον αριθμών (p,q) με $p<q$, η ακόλουθη διαδικασία θα εντωπίσει όλους τους πρώτους $r>q$ τέτοιοι ώστε το $p\cdot q\cdot r$ να είναι αριθμός Carmichael.

Έστω οι ζυγοί διαρέτες (αν υπάρχουν) d του $p\cdot q-1$ με $p<d<p\cdot q-1$ και ελέγχουμε αν $d+1(=r)$ είναι πρώτος, εξαιρούμε το $d=p\cdot q-1$ καθώς θα μας έδινε $r=p\cdot q$. Τότε έχουμε εξασφαλίσει το (iii) και ελέγχουμε λοιπόν αν ισχύουν τα (ii) και (ii).

Το κάνουμε για όλα τα ζευγάρια πρώτων (p,q), όπου $p\cdot q\cdot r<3000$, για πρώτους $r>q$. Όμως λόγω του (3) αφήνουμε εκτός τους συνδυασμούς για τους οποίους ισχύει: $q\equiv 1 \mod p$ (π.χ $(3,7)$).

Καταγράφουμε μόνο τις τιμές του d όπου το r είναι πρώτος. Όπως παρατηρούμε και στον πίνακα από κάτω δεν υπάρχει μικρότερος Carmichael με τρείς παράγοντες από τον 561.

(p, q)	$p \cdot q - 1$	d	r	(i)	(ii)	Carmichael
$(3, 5)$	14	–	–			
$(3, 11)$	32	16	17	yes	yes	$3 \cdot 11 \cdot 17 = 561$
$(3, 17)$	50	–	–			
$(3, 23)$	68	–	–			
$(5, 7)$	34	–	–			
$(5, 13)$	64	16	17	yes	yes	$5 \cdot 13 \cdot 17 = 1105$
$(5, 17)$	84	28	29	yes	yes	$5 \cdot 17 \cdot 29 = 2465$
		42	43	no		
$(5, 19)$	94	–	–			
$(7, 11)$	76	–	–			
$(7, 13)$	90	18	19	yes	yes	$7 \cdot 13 \cdot 19 = 1729$
		30	31	yes	yes	$7 \cdot 13 \cdot 31 = 2821$
$(7, 17)$	118	–	–			
$(11, 13)$	142	–	–			

Το δεύτερο ερώτημα επιλύθηκε με βοήθεια κώδικα.

Κώδικας με σχόλια στο αρχείο:

No31_Smaller_Carmichael_4_Factors.ipynb

Αναφορές